



Password Use

POLICY NUMBER: 9.3.1

EFFECTIVE DATE: 11/01/06

PURPOSE

To establish a standard for creation and use of passwords, the protection of those passwords, and the frequency of change for such passwords to prevent compromise of confidential information.

SCOPE

All personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any State of Georgia facility, has access to the State of Georgia network, or stores any State of Georgia information.

POLICY

Passwords are a primary means to control access to systems and should therefore be selected, used, and managed to protect against unauthorized discovery or usage.

STANDARD

This standard applies to all systems and applications used to process, store, or transfer data with a security categorization of MODERATE or higher.

Password Construction

Strong passwords or strong authentication mechanisms must be used. Strong passwords are defined as having the following characteristics:

- ◆ Are at least eight characters in length.
- ◆ Must contain characters from at least three of the following four types of characters:
 - ◆ English upper case (A-Z)
 - ◆ English lower case (a-z)
 - ◆ Numbers (0-9)
 - ◆ Non-alpha special characters (\$, !, %, ^, ...)
- ◆ Must not contain the user's name
- ◆ Must not contain part of the user's full name

Strong authentication mechanisms use at least two of the three types of authentication mechanisms, what a person knows, what they have, and who they are. Examples of these mechanisms are:

- ◆ What a person knows:
 - ◆ Passwords
 - ◆ PINS
 - ◆ Pictures or graphics
- ◆ What a person has:
 - ◆ The private key associated with a public key certificate
 - ◆ An RSA token associated with an account.

- ♦ Who is a person:
 - ♦ Retina scan
 - ♦ Finger or palm print

Note that these are only examples of methods used for authentication and that many others exist. The emphasis is that two of the three different types of authentication must be used for strong authentication of a user.

Password Protection

All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) should be changed on at least a monthly basis (or with as great a frequency as can be managed without increasing the likelihood that users will write down the password). All user-level passwords (e.g., email, web, desktop computer, etc.) should be changed at least every forty-five days (or with as great a frequency as can be managed without increasing the likelihood that users will write down the password). User accounts that have system-level privileges granted through group memberships or programs should have a unique password from other accounts held by that user. Passwords should not be inserted into email messages or other forms of electronic communication.

Users should not use the same password for State of Georgia accounts as for other non-State of Georgia access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, users should not use the same password for different State of Georgia access needs. For example, a user should select one password for the Engineering systems and a separate password for IT systems. Also, a separate password should be selected to be used for operating system accounts. The exception to this is where a Single Sign On System may control multiple systems.

Users should not share State of Georgia passwords with anyone, including administrative assistants or secretaries. All passwords should be treated as sensitive, confidential information. Users should not write passwords down and store them anywhere in their office. Nor should they store passwords in a file on ANY computer system (including Personal Digital Assistants or similar devices) without encryption. Users should not use the "Remember Password" feature of applications.

If an account or password is suspected of being compromised, the incident should be reported to the appropriate access administrator and the user should change the password. Security administrators should perform periodic, random password audits via automated tools or guessing. If a password is determined during one of these scans, the user should be required to change it.

User Should Not Employ Any Automatic Log-In Actions

State of Georgia information system users should refuse all offers by software and/or Internet sites to automatically login the next time that they access those resources.

Password Sharing Prohibition

Besides the authorized user, passwords should never be shared or revealed to anyone. Temporary or "first use" passwords should be changed the first time that the authorized user accesses the system. To do so exposes the authorized user the responsibility for actions that the other party takes with the password. If users need to share computer resident data, they should use approved network services or any other mechanisms that do not infringe on any policies.

GUIDELINES

Password Uses

Passwords are used for various purposes for State of Georgia Computing Resources. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once) all users should utilize strong passwords.

Password Construction

Strong passwords or strong authentication mechanisms must be used. Strong passwords are defined as having the following characteristics:

- ♦ Are at least eight characters in length.
- ♦ Must contain characters from at least three of the following four types of characters:
 - ♦ English upper case (A-Z)
 - ♦ English lower case (a-z)
 - ♦ Numbers (0-9)
 - ♦ Non-alpha special characters (\$, !, %, ^, ...)
- ♦ Must not contain the user's name
- ♦ Must not contain part of the user's full name

Strong authentication mechanisms use at least two of the three types of authentication mechanisms, what a person knows, what they have, and who they are. Examples of these mechanisms are:

- ♦ What a person knows:
 - ♦ Passwords
 - ♦ PINS
 - ♦ Pictures or graphics
- ♦ What a person has:
 - ♦ The private key associated with a public key certificate
 - ♦ An RSA token associated with an account.
- ♦ Who is a person:
 - ♦ Retina scan
 - ♦ Finger or palm print

Password Protection

All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) should be changed on at least a monthly basis (or with as great a frequency as can be managed without increasing the likelihood that users will write down the password). All user-level passwords (e.g., email, web, desktop computer, etc.) should be changed at least every forty-five days (or with as great a frequency as can be managed without increasing the likelihood that users will write down the password). User accounts that have system-level privileges granted through group memberships or programs should have a unique password from other accounts held by that user. Passwords should not be inserted into email messages or other forms of electronic communication.

Users should not use the same password for State of Georgia accounts as for other non-State of Georgia access (e.g., personal ISP account, option trading, benefits, etc.). Where possible,

users should not use the same password for different State of Georgia access needs. For example, a user should select one password for the Engineering systems and a separate password for IT systems. Also, a separate password should be selected to be used for operating system accounts. The exception to this is where a Single Sign On System may control multiple systems.

Users should not share State of Georgia passwords with anyone, including administrative assistants or secretaries. All passwords should be treated as sensitive, confidential information. Users should not write passwords down and store them anywhere in their office. Nor should they store passwords in a file on ANY computer system (including Personal Digital Assistants or similar devices) without encryption. Users should not use the "Remember Password" feature of applications.

If an account or password is suspected of being compromised, the incident should be reported to the appropriate access administrator and the user should change the password. Security administrators should perform periodic, random password audits via automated tools or guessing. If a password is determined during one of these scans, the user should be required to change it.

User Should Not Employ Any Automatic Log-In Actions

State of Georgia information system users should refuse all offers by software and/or Internet sites to automatically login the next time that they access those resources.

Password Sharing Prohibition

Besides the authorized user, passwords should never be shared or revealed to anyone. Temporary or "first use" passwords should be changed the first time that the authorized user accesses the system. To do so exposes the authorized user the responsibility for actions that the other party takes with the password. If users need to share computer resident data, they should use approved network services or any other mechanisms that do not infringe on any policies.

Application Development

Application developers should ensure their programs contain the following security precautions:

- ◆ Applications should support authentication of individual users, not groups.
- ◆ Applications should not store passwords in clear text or in any easily reversible form.
- ◆ Applications should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

Use of Passwords and Pass phrases for Remote Access Users

Access to the State of Georgia Networks via remote access should be controlled using either a one-time password authentication or a public/private key system with a strong pass phrase. Pass phrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the pass phrase to "unlock" the private key, the user cannot gain access.

Pass phrases are not the same as passwords. A pass phrase is a longer version of a password and is, therefore, more secure. A pass phrase is typically composed of multiple words. Because of this, a pass phrase is more secure against "dictionary attacks". A good pass phrase is relatively long and contains a combination of upper and lowercase letters and

numeric and punctuation characters. All of the rules that apply to passwords apply to pass phrases.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

- ♦ Exceptions must be justified in writing and accepted by the Agency CIO or equivalent.
- ♦ In the case of an information system managed by a third party, the Agency CIO can, in concurrence with the information owner, make a determination that the third party's security controls meet or exceed this standard. This exception must be based on an assessment of the third party's controls and documented in writing. Please see policies 4.2.2, 4.3.1, and 8.1.5 for further information.

TERMS AND DEFINITIONS (see Section 2)